

BIG DATA E VIGILÂNCIA ESTATAL: O Cadastro Base do Cidadão à Luz da Lei Geral de Proteção de Dados

Clarissa Sanglard Hisse

Resumo: *O presente artigo tem por objetivo analisar o tratamento concedido pelo ordenamento jurídico brasileiro aos dados pessoais, com especial atenção à Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18) ao Cadastro Base do Cidadão (criado pelo Decreto nº 10.046/19) – avaliando a compatibilidade entre estes diplomas, bem como os riscos de que esta megabase de dados se converta numa poderosa ferramenta de tecnoautoritarismo estatal. Fundamentando-se em institutos como privacidade, autodeterminação informativa, liberdade de expressão, cidadania e direitos humanos, a LGPD estabeleceu um regime jurídico geral para disciplinar o tratamento de dados de pessoas naturais, tanto por meio físico, quanto por meio digital. O diploma foi responsável por esclarecer e consolidar conceitos e diretrizes indispensáveis para conferir segurança jurídica à matéria tão recente. Apesar do projeto de lei ter sido aprovado por unanimidade pelo Congresso Nacional, após ampla discussão com a sociedade civil, a LGPD sofreu algumas alterações em decorrência de vetos do então presidente Michel Temer e, posteriormente, do presidente Jair Bolsonaro, afrouxando sanções nela previstas e submetendo a Autoridade Nacional de Proteção de Dados à Presidência da República, pelo menos nos primeiros dois anos de seu funcionamento. Além disso, num movimento político-normativo que sugere um descompasso com os princípios estabelecidos pela lei, Bolsonaro assinou o Decreto nº 10.046/2019, que regulamenta e facilita o compartilhamento de dados entre órgãos e entidades da administração pública federal e institui o Cadastro Base do Cidadão – base integradora de dados sobre os cidadãos para compartilhamento entre mais de 50 bases de dados do governo. Causa estranheza o fato do decreto presidencial não incorporar princípios e conceitos trazidos pela lei geral da matéria, desconsiderando e até contrariando preceitos fundamentais do diploma, como o princípio da autodeterminação informativa. Gera ainda mais preocupação a nebulosidade acerca da natureza e da extensão da coleta de dados pessoais para o Cadastro Base, que incluirá, dentre diversos outros, os abrangentes e possivelmente sensíveis “atributos biográficos” e “atributos biométricos”.*

Palavras-chave: Cadastro Base do Cidadão, Lei Geral de Proteção de Dados, Big Data, vigilância, privacidade, tecnoautoritarismo.

1. INTRODUÇÃO

Nas últimas décadas assistimos a um exponencial crescimento do papel da tecnologia em nossas vidas cotidianas, processo que vem transformando com velocidade as formas de sociabilidade num mundo cada vez mais globalizado. As tecnologias de comunicação da informação ganham destaque nesse cenário, revolucionando tanto o dia-a-dia dos cidadãos quanto as estruturas de poder.

As imbricações entre política e comunicação estão sendo rearranjadas na chamada Era da Informação, trazendo novos desafios à implementação de direitos a nível global. Se,

por um lado, podemos desfrutar dos benefícios da imensa ampliação do acesso ao conhecimento e das facilidades promovidas pela digitalização, por outro, temos de estar preparados para lidar com seus potenciais inconvenientes.

Diante de mudanças sociais tão velozes e significativas, é inevitável que surjam lacunas nos ordenamentos jurídicos e que determinadas normas legais se tornem obsoletas e que instrumentos previstos como garantidores de direitos se tornem inadequados ou ineficientes. Com o advento da Internet, temas como o direito à privacidade e ao esquecimento estão se tornando cada vez mais distantes daquilo que se entendia como razoável em outros tempos, exigindo atualização de diplomas normativos, no sentido de tornar a legislação mais moderna e adequar a utilização da tecnologia conforme os princípios constitucionais.

Quando uma grande massa de cidadãos passa a produzir dados sobre si em larga escala, nas mais diversas plataformas digitais, gera-se um produto informacional inédito, cujo potencial ainda está sendo descoberto – e criado. Muito se fala hoje que “os dados são o novo petróleo”, e de fato observa-se que a demanda por serviços de coleta e tratamento de dados cresce a cada dia, fomentando um novo mercado que abrange diversos setores da economia. A tendência à digitalização é clara e veio para ficar, assim como o emprego da *internet das coisas*¹, de modo que parecemos ingressar num estado de vigilância permanente e quase integral, capaz de dissecar nossas vidas por completo.

Algoritmos e inteligência artificial são as palavras da vez na economia digital, especialmente em razão dos sistemas de recomendação personalizada, que operam a partir desse vasto material de dados pessoais fornecidos a todo tempo nos mais diversos aplicativos, redes sociais e demais bancos de dados digitais. O fato dos cidadãos não terem a plena capacidade de controlar as pegadas digitais que produzem acaba gerando uma condição de muita vulnerabilidade, tanto pessoal quanto social.

Em sua obra *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, a pesquisadora norte-americana Shoshana Zuboff, trata das transformações na lógica do sistema capitalista em decorrência das tecnologias digitais. Em sua análise sobre o que chama de capitalismo de vigilância, a autora enfatiza a associação entre mecanismos de predição e de influência de comportamento como uma das principais características dessa nova lógica de acumulação. Segundo ela,

“O capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima disponível e acessível gratuitamente para ser traduzida em dados comportamentais. Embora parte desses dados sejam aplicados para o aprimoramento dos produtos ou serviços, o resto desses dados é transformado em excedente comportamental proprietário, que fomenta processos de produção avançados conhecidos como “inteligência de máquina” e fabrica produtos de predição que antecipam o que você fará agora, em breve e depois. Finalmente, esses produtos de previsão são negociados em um novo tipo de mercado para o que chamo de mercados de comportamento futuro. (...) a dinâmica competitiva desses novos mercados impulsiona os capitalistas de

¹ O termo “Internet das Coisas” se refere a uma revolução tecnológica que tem como objetivo conectar os itens usados do dia a dia à rede mundial de computadores.

vigilância a adquirirem fontes cada vez mais preditivas de excedente comportamental: nossas vozes, personalidade e emoções. Por fim, os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos são adquiridos a partir da intervenção no curso da ação [*state of play*], a fim de estimular, ajustar e persuadir o comportamento na busca de resultados lucrativos. Pressões competitivas produziram essa mudança, na qual processos máqunicos automatizados não apenas conhecem nosso comportamento, mas também moldam nosso comportamento em escala. Com essa reorientação do conhecimento para o poder, não é mais suficiente automatizar os fluxos de informação sobre nós; o objeto agora é nos automatizar. Nessa fase do desenvolvimento do capitalismo de vigilância, os meios de produção estão subordinados a um “meio de modificação comportamental” cada vez mais complexo e abrangente”. (ZUBOFF, 2019, p. 14-15).

Zuboff sugere que as transformações na lógica de acumulação capitalista atual introduzem “meios de modificação comportamental” a partir de “produtos de predição”. Nesse sentido, é a partir do acúmulo de informações extraídas da vigilância contínua sobre nossas ações que os serviços da Internet extraem o “excedente comportamental”, isto é, quaisquer tipos de dados e/ou metadados sob os quais são aplicadas técnicas computacionais inteligentes para se extrair predições de nossas ações futuras. Segundo ela, quanto maior a acuidade preditiva desses sistemas, maior será seu valor de mercado e, por sua vez, maior o potencial de influenciar aquela ação.

Significa dizer que quem controla os dados possui um enorme poder político e econômico nesta nova etapa do capitalismo. Não à toa que empresas como o *Facebook Inc.* e a *Alphabet Inc.* (holding que controla o Google) figuram entre as mais valiosas no mercado global². Por estas razões, inúmeros debates vêm sendo levantados pela sociedade civil sobre os limites ao uso dos dados pessoais, a fim de proteger os cidadãos de eventuais lesões a direitos individuais e coletivos. Escândalos de impacto internacional como os casos do *WikiLeaks*³ e da empresa *Cambridge Analytica*³ fizeram o mundo inteiro voltar os olhos para a importância da segurança da informação e para o potencial explosivo dos dados pessoais que compartilhamos na rede.

O Direito Digital vem então ascendendo em importância e novas legislações e autoridades regulatórias estão sendo criadas no Brasil e no mundo. Neste cenário do *big*

2 <https://www.hardware.com.br/artigos/top-10-empresas-de-tecnologia-mais-valiosas-do-mundo/> ³

Fundada por Julian Assange em 2006, WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis.

3 *Cambridge Analytica, Ltd.* foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral. A empresa protagonizou um escândalo em 2018 por coletar ilegalmente informações pessoais identificáveis de até 87 milhões de usuários do *Facebook*. Os dados foram utilizados para influenciar a opinião de eleitores em vários países para ajudar políticos a influenciarem eleições em seus países.

*data*⁴, em que a coleta significativa de dados pessoais se tornou realidade, bem como a monetização desses ativos para os mais diversos fins econômicos, evidenciou-se a necessidade de regulamentação desses espaços digitais, como forma de assegurar direitos e liberdades fundamentais, como a privacidade e a proteção de dados pessoais.

Estudo da UNESCO⁵, publicado em 2017, considera que as pedras angulares para a promoção de sociedades do conhecimento inclusivas são o acesso à informação e ao conhecimento, a liberdade de expressão, a privacidade e a ética na Internet global. A promoção destes objetivos se constrói a partir dos princípios dos direitos humanos, da abertura, da acessibilidade e da multissetorialidade.

Dilemas a respeito de que tipo de sociedades do conhecimento desejamos construir e pertencer movimentam o cenário global – seja nas vozes de acadêmicos, políticos ou da sociedade civil. Reconhecendo o impacto da Internet e da digitalização para o funcionamento da democracia constitucional tal qual a concebemos, é preciso pensar em formas de governança da Internet capazes de promover ideais democráticos e republicanos neste novo ambiente de sociabilidade e de fluxo de dados.

No Brasil, já contávamos com o Marco Civil da Internet (Lei nº 12.965/2014) e recentemente entrou em vigor a Lei Geral de Proteção de Dados (Lei nº 13.709), que se tornou o principal marco regulatório sobre privacidade e proteção de dados no país. Inspirada em grande medida no regulamento europeu de proteção de dados, a LGPD nasceu após considerável pressão política e comercial para adequação dos negócios às exigências internacionais. Entre as mais celebradas inovações trazidas pela lei, destacam-se o reconhecimento da titularidade dos dados à pessoa natural à qual se referem, e a exigência do consentimento expresso deste titular para o tratamento de seus dados pessoais.

A lei passou por uma longa tramitação no Congresso Nacional, em um processo que atravessou três governos e contou com consultas públicas, debates com a sociedade civil, tendo sido finalmente sancionada em 2018, pelo então presidente Michel Temer.

4 *Big Data*, de acordo com o dicionário Cambridge, se refere a grandes conglomerados de dados produzidos por pessoas que usam a Internet e que só podem ser armazenados, entendidos e usados com a ajuda de ferramentas e métodos especiais. O termo surgiu em 1997 foi utilizado para nomear a quantidade crescente e não estruturada de dados sendo gerados a cada segundo graças às mídias digitais. Atualmente está em desenvolvimento uma área do conhecimento que estuda como tratar, analisar e obter informações a partir destes enormes conjuntos de dados, mesclando técnicas de ciências sociais, matemática, computação e tecnologia da informação.

5 *Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet*. Publicado em 2015 pela Organização das Nações

Unidas para a Educação, Ciência e Cultura. Disponível em: <http://www.unesco.org/new/en/Internetstudy> ⁷

Em razão da pandemia do novo coronavírus o Governo Federal editou a MP nº 959, que, entre outras medidas, prorrogava ainda mais o início da vigência da LGPD, sob a justificativa de conceder mais tempo para adaptação à lei. A Medida Provisória foi aprovada, mas com exclusão desta proposta.

Após longo período de *vacatio legis* e de incertezas a respeito do efetivo início de sua vigência⁷, a LGPD entrou em vigor em setembro de 2020.

No entanto, as sanções previstas na lei passarão a vigorar apenas a partir de 1º de agosto de 2021, em virtude da aprovação da Lei nº 14.010/20, que trata do Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET). A mudança teria o objetivo de não onerar as empresas, que já enfrentariam enormes dificuldades técnicas e econômicas por causa da pandemia do novo coronavírus. Ainda assim, o adiamento ainda se demonstra especialmente sensível por ocorrer justo quando a digitalização se intensifica pelo necessário isolamento social.

Paralelamente a esse processo, em outubro de 2019, durante o período de vacância da lei, o presidente Jair Bolsonaro editou o decreto nº 10.046, criando o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. A medida, que foi tomada e aprovada sem consultas e debates públicos, institui uma megabase de dados sem precedentes na história do país, que pode criar uma ferramenta de vigilância poderosa com um potencial devastador para a privacidade dos cidadãos brasileiros. Trata-se de uma integração entre mais de 50 bases de dados do governo, que inclui desde CPF às informações sobre emprego, saúde e até dados biométricos.

A compatibilidade entre os dois textos normativos é controversa: além de determinados dispositivos parecerem contrariar a LGPD – como os princípios da finalidade, da necessidade e da autodeterminação informativa, a própria terminologia utilizada pelo decreto para definir dado pessoal não é a mesma da lei geral. Além disso, o decreto prevê poucos mecanismos para controle público dessa vigilância estatal.

2. A SISTEMÁTICA DA PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL

No ordenamento jurídico pátrio, o celebrado Marco Civil da Internet (Lei nº 12.698/2014) consagrou o acesso à Internet como elemento essencial ao exercício da cidadania e estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Antes de virar lei, a proposta foi lançada pela Secretaria de Assuntos Legislativos do Ministério da Justiça, em outubro de 2009, possibilitando um amplo debate junto à sociedade civil.

O Marco Civil da Internet, que tem por objetivo central disciplinar a relação entre empresas operadoras de produtos ou serviços associados à Internet e os seus respectivos usuários dentro do território nacional, fundamenta-se essencialmente nos princípios da liberdade de expressão, da privacidade e da neutralidade da rede.

O diploma inovou em diversos aspectos, consagrando em seu art. 3º os princípios que norteiam o uso da Internet no Brasil, dentre os quais se destaca para este estudo o inciso III, que trata da proteção dos dados pessoais:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

- I** - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II** - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;**
- IV** - preservação e garantia da neutralidade de rede;
- V** - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI** - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- VII** - preservação da natureza participativa da rede;
- VIII** - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

A proteção dos dados pessoais também foi disciplinada pelos arts. 7º e 16 do mesmo diploma, assegurando que sua coleta seja condicionada ao consentimento livre, expresso e informado do usuário (ou nas hipóteses previstas em lei), bem como exigindo publicidade e clareza em relação às políticas de uso e privacidade, *in verbis*:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

(...)

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

- a) justifiquem sua coleta;
- b) não sejam vedadas pela legislação; e
- c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; **XI** - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou **II** - dos dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Reconhecendo a importância de tratar em diploma próprio o tratamento dos dados pessoais no Brasil, a fim de salvaguardar direitos fundamentais, em agosto de 2018 foi promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/18) – suprimindo uma lacuna legislativa por uma norma geral sobre o tema, que até então dependia de regras e previsões pontuais e esparsas.

Sua promulgação foi consequência de impacto exercido pelo mercado internacional, em especial em decorrência da entrada em vigor em maio de 2018 do regulamento de proteção de dados da União Europeia – *General Data Protection Regulation* (GDPR), no qual a lei brasileira é amplamente inspirada.

A Lei Geral de Proteção de Dados Pessoais dispõe sobre o tratamento de dados de pessoas naturais, tanto por meio físico, quanto por meio digital, reconhecendo a finalidade da tutela dessas informações para a proteção dos direitos humanos e da cidadania. Logo em seu art. 2º, a LGPD elenca um rol de direitos que fundamentam a tutela da proteção de dados pessoais, *in verbis*:

Art. 2º A disciplina da proteção de dados pessoais tem como **fundamentos**:

- I** - o respeito à privacidade;
- II** - a autodeterminação informativa;
- III** - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV** - a inviolabilidade da intimidade, da honra e da imagem;
- V** - o desenvolvimento econômico e tecnológico e a inovação;
- VI** - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII** - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD protege situações que concernem às operações de “tratamento de dados”, elencando um extenso rol de atividades que se enquadram na categoria. Conforme disciplina o inciso X do seu art. 5º, considera-se tratamento de dados “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

O mesmo dispositivo legal trouxe diversos conceitos importantíssimos à aplicação da lei, tais como *dado pessoal*, *dado pessoal sensível*, *dado anonimizado*, *banco de dados*, *titular de dado pessoal* e *consentimento*.

Para os fins dessa lei, considera-se *dado pessoal* toda a informação relacionada à pessoa natural identificada ou identificável. *Dado pessoal sensível*, por sua vez, é aquele que traz informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, ou referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.

Já os *dados anonimizados* são aqueles cujos titulares são impossíveis de identificar utilizando meios técnicos razoáveis e disponíveis na ocasião do seu tratamento. O dado anonimizado não será considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Uma das principais novidades trazidas pela lei, considerada um grande avanço pelos ativistas do direito digital, diz respeito à *titularidade* dos dados pessoais: a legislação reconhece sua titularidade à pessoa natural a quem se referem, exigindo seu *consentimento* expresso para que sejam objeto de tratamento. Tal consentimento deve ser uma manifestação livre, informada e inequívoca pela qual o titular concorde com o tratamento de seus dados pessoais para uma finalidade determinada – devendo ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Consagra-se, nesse sentido, o princípio da autodeterminação informativa, que consiste na soberania do titular sobre o fornecimento de dados pessoais. Trata-se de um dos fundamentos do referido diploma legal, e nada mais é do que a ideia de que o indivíduo titular de dados pessoais deve ter controle, ou ao menos plena transparência, sobre a destinação dada às suas informações pessoais, bem como sobre as metodologias utilizadas para tanto.

A ideia de autodeterminação informativa se articula com uma nova concepção de privacidade, que escapa à noção tradicional de proteção contra intromissões indesejadas na esfera pessoal, se comunicando mais com uma noção de boa-fé, com o dever de prestar informações e com os princípios da necessidade e da finalidade.

Ampliou-se, assim, a exigência por uma linguagem contratual mais clara, em especial em relação ao instrumento utilizado para que o titular forneça seu consentimento. O titular passa a ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva em relação à finalidade específica do tratamento, bem como acerca de sua forma e duração, entre outros:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I** - finalidade específica do tratamento;
- II** - forma e duração do tratamento, observados os segredos comercial e industrial;
- III** - identificação do controlador;
- IV** - informações de contato do controlador;
- V** - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI** - responsabilidades dos agentes que realizarão o tratamento; e
- VII** - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Muitos juristas têm comparado o impacto deste marco legal ao Código de Defesa do Consumidor de 1991, que remodelou tanto o comportamento de empresas e consumidores como os costumes e a jurisprudência nos tribunais, reconhecendo uma série de direitos aos cidadãos frente ao poder econômico. Mesmo antes de entrar em vigor, a LGPD já vinha movimentando o mercado de *data driven economy*⁶, inclusive no ramo do direito digital, com um crescimento da procura por serviços de *data protection compliance*⁷, a fim de adequar as empresas à nova legislação.

Neste cenário, a LGPD disciplina os direitos conferidos aos titulares dos dados pessoais, que poderão requisitar: (i) informações para confirmar a existência de tratamento dos seus dados; (ii) acesso aos seus dados; (iii) solicitar correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados (desnecessários, excessivos ou em desconformidade com a lei); (v) portabilidade dos dados; (vi) eliminação de dados pessoais tratados com o consentimento do titular (exceto nas hipóteses previstas no art. 16¹⁰); (vii) informações sobre entidades com as quais os dados foram compartilhados; (viii) informações sobre a possibilidade de não fornecer consentimento e suas consequências; (ix) revogar o consentimento.

Com o intuito de limitar as atividades de tratamento de dados, em seu art. 6º, a LGPD disciplina que as atividades de tratamento de dados deverão ser norteadas pela boa-fé e pelos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, *in verbis*:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

6 “Data Driven Economy” diz respeito às transformações do capitalismo rumo a uma economia norteada pelo tratamento de dados.

7 “Data Protection Compliance” é a necessidade de adequação a fim de cumprir os requisitos legais referentes ao tratamento de dados.

- VII - segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- VIII - prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- IX - não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- X - responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Em relação ao tratamento dos dados pessoais sensíveis, destacam-se os princípios da finalidade e da não discriminação. De acordo com o princípio da finalidade, os propósitos para os quais houver tratamento de dados devem ser explícita e previamente informados ao titular, excluída a possibilidade de utilização posterior para outro fim. Com base nesse princípio fundamenta-se a restrição da transferência de dados pessoais a

¹⁰ Art. 16. **Os dados pessoais serão eliminados após o término de seu tratamento**, no âmbito e nos limites técnicos das atividades, **autorizada a conservação para as seguintes finalidades:**

- I - cumprimento de obrigação legal ou regulatória pelo controlador;
- II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

terceiros, bem como representa um importante critério para valorar a razoabilidade ou abusividade da utilização dos dados.

Trata-se de uma medida para limitar e dar objetividade ao tratamento de dados pessoais, definindo o que será considerado como finalidade legítima do tratamento. Ainda assim, a norma prevê que, para algumas categorias de dados especialmente sensíveis, a única finalidade admissível é o interesse do titular.

O princípio da não discriminação, por sua vez, veda a utilização de dados pessoais para fins discriminatórios ilícitos ou abusivos. Esse princípio ganha relevância diante dos avanços da inteligência artificial baseada em algoritmos, capazes de operar técnicas de pesquisa social para categorizar e segmentar indivíduos e grupos sociais com base em programações muitas vezes discriminatórias.

Interessante atentar para o fato de o legislador ter optado por relacionar o termo “uso discriminatório” às qualidades de ilicitude e abusividade, de modo que não está vedado todo tipo de tratamento discriminatório de dados – desde que não se enquadre nestas hipóteses. Todavia, há que se questionar se esse tipo de tratamento poderia também ser realizado em relação aos dados pessoais sensíveis, considerando suas características personalíssimas.

O jurista italiano Stefano Rodotà sustenta que formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação: segundo o autor, “[...] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como ‘a proteção de escolhas de vida contra qualquer forma de controle público e estigma social’” (RODOTÀ, 2008, p.12).

Por essas razões, a fim de conferir maior proteção aos titulares de dados sensíveis, o GDPR qualificou de maneira mais restrita o consentimento do titular dos dados sensíveis, passando a exigir que, além de expressa, a manifestação consentida deve ser livre, explícita, inequívoca, informada e específica. Neste ponto, a legislação nacional não seguiu o modelo europeu, permitindo que haja tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, quando for indispensável para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos – conforme disciplina o art. 11, II, b, LGPD – além de outras hipóteses que se referem, em grande medida, a interesses públicos.

Neste último caso, o consentimento do titular dos dados sensíveis, seja genérico, seja específico, ficaria dispensado em decorrência de uma ponderação de interesses realizada pela lei, aprioristicamente, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular, ainda que estes tenham qualidade de direito fundamental.

O Supremo Tribunal Federal reconheceu a existência do direito fundamental à proteção de dados no bojo da ADI nº 6.387. A Corte entendeu que o direito fundamental à proteção de dados possui conteúdo autônomo que justifica a sua tutela constitucional, mesmo que esteja conectado aos direitos à privacidade, intimidade e sigilo de dados (art. 5º, incisos X e XII, CF/88). No mesmo sentido, já tramita no Congresso Nacional proposta de emenda constitucional que visa a incluir a proteção de dados pessoais entre os direitos fundamentais no Brasil (PEC nº 17/2019).

Por fim, mas não menos importante, a Lei Geral de Proteção de Dados Pessoais instituiu a Autoridade Nacional de Proteção de Dados, tendo o condão de assumir a posição de autoridade máxima para fiscalizar e regulamentar a proteção de dados no país. Num raro consenso entre ativistas do direito digital e representantes do setor privado, os debates legislativos apontavam a imperiosa necessidade de que a entidade tivesse autonomia em relação ao Poder Executivo, a fim de garantir uma atuação mais isenta de pressões políticas.

A ANPD pode ser considerada o coração da LGPD, pois acumula as funções normativa, coordenativa, fiscalizatória, sancionatória e educativa. A Autoridade tem a responsabilidade de guiar a sociedade numa transformação que não é apenas jurídica, mas também cultural. Além disso, ela também é responsável por fiscalizar o tratamento de dados operado pelo próprio poder público.

Pela sua relevância, e adotando padrões internacionais, o legislador brasileiro havia optado por arquitetar uma Autoridade Nacional de Proteção de Dados Pessoais baseada

em ideal de independência e autonomia – inclusive orçamentária, e vinculada à administração pública indireta, nos moldes de uma agência reguladora.

Todavia, apesar da LGPD ter sido aprovada por unanimidade no Congresso Nacional, todo o texto referente à ANPD foi vetado pelo então presidente Michel Temer, devido a uma suposta inconstitucionalidade formal consistente em vício de iniciativa. Posteriormente, no apagar das luzes de seu governo, Temer editou a Medida Provisória nº 869/2018, criando finalmente a ANPD, mas alterando substancialmente sua natureza jurídica: a Autoridade passou a ficar vinculada à Presidência da República.

O texto da MP foi submetido a uma Comissão Mista entre Câmara e Senado, já no contexto de uma nova legislatura, com outro equilíbrio de forças políticas. O Legislativo conseguiu reestabelecer algumas prerrogativas da ANPD que constavam do texto original e que haviam ficado de fora da MP, e quanto à independência, a solução foi alterar o texto para dotar a ANPD de uma natureza jurídica transitória:

Art. 55-A. Fica criada, **sem aumento de despesa**, a Autoridade Nacional de Proteção de Dados (ANPD), **órgão da administração pública federal, integrante da Presidência da República**. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

Após parecer da Comissão Mista, o novo texto foi sancionado com vetos pelo presidente Jair Bolsonaro, e convertido na Lei 13.853/2019. O texto final aprovado derrubou algumas sanções que poderiam ser aplicadas pela ANPD. Entre elas, estavam previstas a interrupção parcial do funcionamento do banco de dados (por seis meses, prorrogável por igual período) e a proibição parcial e total de atividades relacionadas ao tratamento de dados.

Outro item que ficou de fora previa a aplicação de sanções a órgãos públicos. Também foi vetada uma garantia ao cidadão que fizesse solicitações via Lei de Acesso à Informação, que tinha por objetivo evitar possíveis retaliações à prática de questionamentos por maior transparência.

Outro importante ponto da lei que foi vetado por Bolsonaro diz respeito à tutela das decisões automatizadas. O texto original da lei disciplinava que a revisão de decisões automatizadas deveria ser feita por pessoas naturais, mas essa exigência caiu com o veto, de modo que, quando solicitada, a revisão também poderá ser feita de forma automatizada. A revisão de decisões automatizadas por pessoas naturais tem o objetivo de evitar injustiças e discriminações algorítmicas, muitas vezes camufladas pela opacidade desses sistemas.

Atualmente, a LGPD já se encontra em vigor, após um período de incertezas, em especial pelas tentativas de prorrogação em decorrência da pandemia do novo coronavírus. A ANPD foi efetivamente criada pelo governo federal com o Decreto nº 10.474, de 26 de agosto de 2020. Todavia, a Autoridade permanece limitada em suas medidas de *enforcement* representadas pelas suas sanções, que apenas passarão a vigorar em agosto de 2021.

Dentre os cinco nomes indicados para o Conselho Diretor da ANPD por Bolsonaro, três são membros do Exército brasileiro, em sua maioria com experiência limitada no tema da proteção de dados enquanto direito autônomo⁸. Todos os três foram designados para os mandatos com maior tempo de duração. A Coalizão Direitos na Rede e a AccessNow enviaram carta-denúncia para Comissão Europeia, Conselho da Europa e Global Privacy Assembly, alertando os órgãos internacionais sobre os riscos das indicações de militares para o Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD)⁹.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) apresentou um relatório com recomendações pertinentes à Autoridade Nacional de Proteção de Dados, sugerindo que o governo brasileiro trabalhe para garantir a independência do órgão.

3. O CADASTRO-BASE DO CIDADÃO E O DECRETO Nº 10.046/2019

Em outubro de 2019, o presidente Jair Bolsonaro assinou o Decreto nº 10.046/2019, regulamentando o compartilhamento de dados entre órgãos e entidades da administração pública federal e instituindo o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. A nova regulamentação reduz as barreiras ao compartilhamento e ao cruzamento de bancos de dados da administração pública federal, tendo por justificativa sanear problemas como a duplicidade de informações e inconsistências em bases de dados públicas, a fim de facilitar e aprimorar a gestão de políticas públicas, bem como ampliar o acesso do cidadão a serviços governamentais.

A simplificação dos mecanismos de compartilhamento e cruzamento de dados pela administração pública já havia sido objeto do Decreto nº 8.789/2016, assinado pelo expresidente Michel Temer, sob o argumento de modernizar a administração pública e promover maior eficiência na gestão de políticas.

O novo decreto revoga expressamente o anterior, mas mantém e aprofunda o padrão de facilitação do compartilhamento e intercâmbio de dados por ele instituída – além de trazer novidades alarmantes para a proteção de dados pessoais no território nacional, conforme abordaremos a seguir.

⁸ <http://direitosnarede.org.br/2020/10/16/anpd-militarizada-risco-para-a-protecao-de-dados-pessoais/>

⁹ <https://direitosnarede.org.br/2020/11/10/cdr-e-access-now-enviam-carta-denuncia-para-comissao-europeia-conselho-da-europa-eglobal-privacy-assembly/>

Em primeiro lugar, o novo decreto amplia abrangência da esfera governamental: apesar de ambos os regulamentos tratarem da governança no compartilhamento de dados no âmbito da administração pública federal, o novo decreto não mais se restringe aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional, incluindo também os demais Poderes da União – os Poderes Legislativo e Judiciário.

As finalidades lícitas previstas para o compartilhamento de dados também foram significativamente ampliadas. Enquanto a regulamentação anterior previa como finalidade a formulação, implementação, avaliação, oferta e análise de políticas públicas, serviços públicos e benefícios sociais e fiscais, o novo decreto passou a incluir a finalidade genérica e abrangente de “aumentar a qualidade e eficiência das operações internas da administração pública federal”. Tal ampliação parece extrapolar as hipóteses elencadas no rol de bases legais do art. 7º da Lei Geral de Proteção de Dados, que os restringe aos dados necessários à execução de políticas públicas.

A extensão semântica do termo “dados cadastrais” também foi ampliada pelo novo decreto: para além da lista não exaustiva de identificadores cadastrais de pessoas físicas e jurídicas junto aos órgãos públicos, tais como nome civil, data de nascimento, filiação, endereço, CPF/CNPJ e PIS – já prevista na regulamentação anterior – incluem-se agora nesse conceito os denominados “atributos biográficos”, conforme disciplina o art. 2º do decreto:

Art. 2º Para fins deste Decreto, considera-se:

I - atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;

II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

III - dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos, tais como: a) os atributos biográficos;

- b) o número de inscrição no Cadastro de Pessoas Físicas - CPF;
- c) o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
- d) o Número de Identificação Social - NIS;
- e) o número de inscrição no Programa de Integração Social - PIS;
- f) o número de inscrição no Programa de Formação do Patrimônio do

Servidor Público - Pasep;

- g) o número do Título de Eleitor;
- h) a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação

Nacional de Atividades Econômicas - CNAE; e

- i) outros dados públicos relativos à pessoa jurídica ou à empresa individual;

Os denominados “atributos biográficos” são descritos como “dados de pessoa natural relativos aos fatos da sua vida”, os quais são apresentados num rol não taxativo no texto normativo, compreendendo, mas não se limitando às informações relativas a “nome civil

RBHD, Rio de Janeiro, v.1, n. 2, Dossiê Temático 2, p. 100-125, jan./jun., 2021

ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios”. O uso da expressão “fatos da vida” abre excessivamente o campo semântico da norma, em razão da vagueza e indeterminação do termo, ampliando sobremaneira a diversidade de dados pessoais que podem vir a ser acomodados pelo dispositivo – o que pode vir a incluir dados pessoais sensíveis.

Compreender a extensão de tais conceitos é fundamental para analisar a dimensão e as implicações do Cadastro Base do Cidadão – uma base integradora e plataforma de interoperabilidade que possibilita o intercâmbio de dados entre esta base e outras bases temáticas. O decreto anterior já permitia o compartilhamento automático de dados cadastrais, mas a nova regulamentação amplia em diversos níveis a extensão desse compartilhamento, como veremos a seguir.

Conforme prevê o art. 18 do novo decreto, inicialmente o Cadastro Base do Cidadão será composto de dados cadastrais e atributos biográficos e biométricos provenientes da base de dados temática do Cadastro de Pessoa Física – CPF. Posteriormente, essa base integradora será acrescida de informações provenientes de outras bases temáticas governamentais que contenham dados biográficos e biométricos. Apenas os atributos genéticos (além dos dados protegidos por sigilo fiscal sob gestão da Secretaria Especial da Receita Federal do Brasil do Ministério da Economia, conforme § 2º do art. 1º) ficam excluídos da sua incidência. *In verbis*:

Art. 18. A base integradora será, inicialmente, disponibilizada com os dados biográficos que constam da base temática do CPF.

§ 1º Os atributos biográficos e cadastrais que inicialmente comporão a base integradora serão, **no mínimo**, os seguintes:

- I - número de inscrição no CPF;
- II - situação cadastral no CPF;
- III - nome completo;
- IV - nome social;
- V - data de nascimento;
- VI - sexo;
- VII - filiação;
- VIII - nacionalidade;
- IX - naturalidade;
- X - indicador de óbito;
- XI - data de óbito, quando cabível; e
- XII - data da inscrição ou da última alteração no CPF.

§ 2º A base integradora será acrescida de outros dados, provenientes de bases temáticas, por meio do número de inscrição do CPF, atributo chave para a consolidação inequívoca dos atributos biográficos, biométricos e cadastrais.

(...)

§ 6º Excetuam-se do disposto no § 2º os atributos genéticos.

Além do Cadastro Base – que pretende ser uma base de referência de informações sobre cidadãos para os órgãos e entidades do Poder Executivo federal – o decreto estabelece normas para o compartilhamento de dados que não estejam abrangidos em seu escopo ou que ainda não estejam integrados a ele. Foram previstos três níveis de compartilhamento destes dados, de acordo com sua classificação: dados *abertos*,

restritos ou *específicos* – cuja classificação fica a cargo do gestor do respectivo banco de dados, que deverá seguir as orientações e diretrizes determinadas pelo *Comitê Central de Governança de Dados*, também instituído pelo novo decreto.

Os dados abertos, também chamados de dados de amplo compartilhamento, são considerados públicos e poderão ser compartilhados sem necessidade de autorização do gestor e catalogados no Portal Brasileiro de Dados Aberto¹⁰. Já os dados de compartilhamento restrito e específico são protegidos por algum tipo de sigilo: os dados restritos serão compartilhados mediante solicitação, de acordo com regras que serão estabelecidas pelo Comitê, todavia, não há restrição à sua retransmissão a outros órgãos e entidades previstos no art. 1º do decreto, exceto se expressamente previsto na autorização do gestor; os dados específicos, por sua vez, também serão compartilhados mediante solicitação, porém, apenas com determinados órgãos público, quando houver previsão legal, conforme autorização e requisitos definidos pelo gestor. Além disso, os dados de conteúdo específico não poderão ser retransmitidos ou compartilhados com outros órgãos e entidades, salvo autorização expressa do gestor.

O Comitê Central de Governança de Dados é outra novidade significativa trazida pelo decreto: composto apenas por representantes da administração pública federal, o Comitê tem competência deliberativa sobre uma série de regras, orientações, diretrizes, parâmetros, controvérsias e decisões relativas à gestão do Cadastro Base e dos níveis de compartilhamento de dados, vide os arts. 21 e 22 do decreto:

Art. 21. Fica instituído o Comitê Central de Governança de Dados, a quem compete deliberar sobre:

- I** - as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico, e a forma e o meio de publicação dessa categorização, observada a legislação pertinente, referente à proteção de dados pessoais;
- II** - as regras e os parâmetros para o compartilhamento restrito, incluídos os padrões relativos à preservação do sigilo e da segurança;
- III** - a compatibilidade entre as políticas de segurança da informação e as comunicações efetuadas pelos órgãos e entidades de que trata o art. 1º, no âmbito das atividades relativas ao compartilhamento de dados;
- IV** - a forma de avaliação da integridade, da qualidade e da consistência de bases de dados derivadas da integração de diferentes bases com o Cadastro Base do Cidadão;
- V** - as controvérsias sobre a validade das informações cadastrais e as regras de prevalência entre eventuais registros administrativos conflitantes, quando ocorrer o cruzamento de informações entre bases de dados do Cadastro Base do Cidadão;
- VI** - as orientações e as diretrizes para a integração dos órgãos e das entidades de que trata o art. 1º com o Cadastro Base do Cidadão;
- VII** - a inclusão, na base integradora do Cadastro Base do Cidadão, de novos dados provenientes das bases temáticas, considerada a eficiência técnica e a economicidade;
- VIII** - a escolha e aprovação das bases temáticas que serão integradas ao Cadastro Base do Cidadão e a definição do cronograma de integração, em comum acordo com os gestores de dados;

¹⁰ <http://dados.gov.br/>

- IX** - as propostas relativas à estratégia para viabilizar, econômica e financeiramente, o Cadastro Base do Cidadão no âmbito do setor público; **X** - a instituição de subcomitês técnicos permanentes ou temporários, para assessorá-lo em suas atividades;
- XI** - a instituição de outros cadastros base de referência do setor público de uso obrigatório pelos órgãos e entidades de que trata o art. 1º; e **XII** - seu regimento interno.

Art. 22. O Comitê Central de Governança de Dados é composto por representantes dos seguintes órgãos e entidade:

- I** - dois do Ministério da Economia, dentre os quais um da Secretaria Especial de Desburocratização, Gestão e Governo Digital, que o presidirá, e um da Secretaria Especial da Receita Federal do Brasil;
- II** - um da Casa Civil da Presidência da República;
- III** - um da Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União;
- IV** - um da Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República;
- V** - um da Advocacia-Geral da União; e **VI** - um do Instituto Nacional do Seguro Social.

Como já mencionado, será o responsável pela definição de parâmetros de classificação para os bancos e bases de dados, bem como estabelecerá regras para o compartilhamento de dados restritos. Além disso, ao Comitê também será incumbida a avaliação das políticas de segurança da informação dos órgãos e entidades relativos às atividades de compartilhamento de dados.

Também compete ao Comitê a definição de diretrizes para integração de órgãos e entidades ao Cadastro Base, bem como a inclusão de outras bases temáticas a esta base integradora. O Comitê fica ainda responsável por instituir outros cadastros base de referência do setor público e de uso obrigatório pelos órgãos e entidades, sem qualquer restrição acerca da finalidade do tratamento desses dados.

A partir desta breve exposição acerca das novidades trazidas pela nova regulamentação, observa-se que a ampliação do acesso e do compartilhamento de dados pessoais pelo poder público não veio acompanhada das respectivas garantias necessárias à segurança da informação e à proteção dos dados pessoais – salvo aqueles dados protegidos por sigilo fiscal.

Em relação ao Comitê Central de Governança de Dados, é questionável que o decreto tenha lhe conferido poderes tão significativos em relação às diretrizes do processamento de dados pessoais sem que haja qualquer participação de representantes da sociedade civil. Desse modo, a elaboração de dispositivos essenciais à proteção de dados pessoais fica submetida a uma instância não participativa com caráter infralegal.

O que mais causa estranhamento, todavia, é o fato do decreto sequer incorporar princípios e conceitos consolidados pela recente Lei Geral de Proteção de Dados, contrariando a tendência expressa pelo legislador de conferir unidade e coesão às normas relativas ao tratamento de dados pessoais, a fim de melhor proteger o cidadão e

a coletividade de eventuais abusos. O atual decreto ignora termos centrais para a compreensão da matéria, que foram normatizados pela referida lei, tais como “dados pessoais”, optando pelo uso de expressões estranhas aos regimes de proteção de dados, como “atributos biográficos” e “atributos biométricos” – sugerindo um movimento de resistência aos princípios que norteiam regime de proteção de dados trazido pelo diploma legal.

Não obstante, o decreto não desconsidera por completo a LGPD, chegando a mencioná-la entre as diretrizes para o compartilhamento de dados, conforme disciplina seu art. 3º:

Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:

I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo receptor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;

(...)

V - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; e

VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018.

De fato, como já mencionado anteriormente, a LGPD prevê o tratamento e o uso compartilhado de dados pessoais pela administração pública para fins de políticas públicas, conforme disciplina o Capítulo IV da lei. Assim, o Decreto nº 10.046/2019 regulamenta e procedimentaliza o compartilhamento já previsto, todavia, em diversos pontos ele parece o fazer à revelia das diretrizes e dos princípios que estruturam o regime de proteção de dados consolidado pela LGPD.

Disciplina a LGPD que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deve atender ao princípio da finalidade, sempre na persecução do interesse público e respeitando suas competências e atribuições legais. A finalidade específica do uso compartilhado de dados pessoais pelo poder público diz respeito à execução de políticas públicas e deve respeitar os princípios de proteção de dados pessoais elencados no art. 6º da LGPD, dentre os quais se destacam: finalidade, adequação, necessidade, livre acesso ao titular e transparência. Vide os arts. 23 e 26 da LGPD:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), **deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público,**

com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender **a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas,** respeitados os **princípios de proteção de dados pessoais elencados no art. 6º** desta Lei.

A compatibilidade entre os dois textos normativos é controversa: não apenas determinados dispositivos parecem contrariar a lei geral, como a própria diretriz do mais amplo compartilhamento que fundamenta o decreto presidencial e a criação do Cadastro Base do Cidadão desafiam os princípios da necessidade e da finalidade.

Apenas os dados de compartilhamento específico parecem se enquadrar nas prerrogativas legais, vez que se trata de dados protegidos por sigilo e apenas órgãos e entidades específicos podem acessá-los, e tão somente nas hipóteses e para os fins previstos em lei.

Tanto o compartilhamento amplo como o restrito extrapolam as hipóteses legais, porquanto seu acesso não exige quaisquer justificativas mais contundentes acerca da adequação, necessidade e finalidade do acesso para a realização de políticas públicas. Além disso, os dados são coletados sem que seus titulares tenham sido informados de maneira clara e precisa acerca dos possíveis tratamentos a que serão submetidos, excedendo a finalidade que teria motivado sua coleta em primeiro lugar. Fica então comprometida a garantia que de os dados pessoais fornecidos serão tratados tão somente para os fins específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior e inconforme.

Resta então o questionamento acerca dos riscos de um governo mais bem informado sobre seus cidadãos – individual e coletivamente. Os princípios da autodeterminação informativa e da privacidade, consagrados na Lei Geral de Proteção de Dados, tem justamente o condão de evitar possíveis abusos no uso, tratamento e compartilhamento de dados pessoais, limitando seu acesso tanto por pessoas jurídicas de direito público quanto privado a fim de resguardar os direitos fundamentais de seus titulares.

Princípios como estes não se limitam a proteger a vida íntima dos cidadãos, como são essenciais para o livre desenvolvimento e a autodeterminação dos indivíduos – fomentando a construção de uma sociedade mais livre e democrática. Os sistemas de vigilância têm mudado de forma e representam hoje um grande desafio aos regimes democráticos: a Internet e a digitalização da vida cotidiana abrem caminhos para um controle excessivo da sociedade, seja pela atuação dos poderes constituídos, seja pelas mãos do capital.

Diversos estudos¹¹ têm sido feitos acerca da influência das redes sociais em pleitos eleitorais, e uma das maiores preocupações dos especialistas diz respeito à utilização de *big data* para o perfilamento algorítmico de grupos sociais para o direcionamento de conteúdo – associado à utilização de estratégias de desinformação.

O perfilamento consiste na construção de modelos (estatísticos) a partir de grandes quantidades de dados de muitos indivíduos, após o que os próprios perfis podem ser explorados para obter novas informações sobre indivíduos específicos. Esse tipo de tecnologia tem sido muito utilizado comercialmente para a publicidade de modo geral, todavia, há que se ter cautela com a utilização de mecanismos que tenham o intuito de moldar o comportamento social, como no caso da tentativa de manipulação da opinião pública.

A instituição do Cadastro Base do Cidadão, fundada na busca do mais amplo compartilhamento de dados pessoais – ainda que sigilosos por força da lei ou da Constituição – aponta para uma possibilidade inédita de perfilamento da população, ao visar à consolidação de atributos cadastrais, biométricos e biográficos numa única base de dados integradora. Na Era da Informação em vivemos, na qual os dados têm sido considerados “o novo petróleo”, isso garante um enorme poder ao Estado em face do indivíduo, ampliando sua possibilidade de vigilância, discriminação e controle. A situação se agrava ainda mais ao mitigar a possibilidade de controle do titular sobre quem e para qual finalidade acessa seus dados – e contraria inequivocamente a vontade do legislador com a mais recente Lei Geral de Proteção de Dados.

A cidadania fica exposta com esse desequilíbrio de poder entre o Estado e o indivíduo, que passa a estar mais sujeita às arbitrariedades de um governo autoritário. Esse movimento de criação de base de dados integradora estatal contraria também o conceito de “separação informal dos poderes”¹², segundo o qual o Estado não deveria ser considerado uma entidade única para fins de coleta e utilização de dados pessoais, mas uma pluralidade de entes que não compartilham entre si tais informações – salvo em casos estritamente necessários à finalidade informada no momento da coleta e respeitadas as competências e previsões legais.

Nesse sentido, na década de 1970 os escritores Malcom Warner e Mike Stone já apontavam os riscos da criação de um arquivo nacional integrado de dados pessoais: *Conceda ao administrador do governo ou de empresas o uso de um arquivo nacional integrado da população [...] e você lhes terá proporcionado uma poderosa ferramenta de interferência na vida privada, para manipular, para vender mais, para condicionar, para coagir.* (WARNER; STONE, 1970, p. 124).

Essa tão perigosa assimetria de informação – e, por conseguinte, de poder – já está desenhada pelo Decreto assinado pelo presidente Jair Bolsonaro: enquanto o Estado

¹¹ <https://observa2018.com.br/>

¹² Tribunal Constitucional Alemão (Bundesverfassungsgericht) cunhou o conceito de separação informacional de poderes, na decisão sobre o censo populacional na década de 80. RBHD, Rio de Janeiro, v.1, n. 2, Dossiê Temático 2, p. 100-125, jan./jun., 2021

reúne, praticamente sem restrições, uma enorme e variada quantidade de dados pessoais (coletados no âmbito das mais diversas políticas públicas), o titular destes dados fica cada vez menos ciente da dimensão das informações que o Estado possui sobre si, bem como sobre a destinação que dará a elas.

Vale mencionar que já há três Projetos de Decreto Legislativo visando sustar seus efeitos: PDL 661/2019, PDL 675/2019 e PDL 673/2019. Os autores destes projetos argumentam, em síntese, que o decreto presidencial extrapola o poder regulamentar conferido ao Poder Executivo, bem com a incompatibilidade de suas normas com dispositivos da Constituição Federal e da Lei Geral de Proteção de Dados.

Além disso, em janeiro de 2021, ao Conselho Federal da Ordem dos Advogados do Brasil ajuizou, no Supremo Tribunal Federal, a Ação Direta de Inconstitucionalidade nº 6649, contra o Decreto 10.046/2019 da Presidência da República. Segundo a OAB, de acordo com as medidas previstas na norma, está sendo construída uma ferramenta de vigilância estatal “extremamente poderosa”, que inclui informações pessoais, familiares e trabalhistas básicas de todos os brasileiros, mas também dados pessoais sensíveis, como dados biométricos, que podem ser coletados para reconhecimento automatizado, como a palma da mão, as digitais, a retina ou a íris, o formato da face, a voz e a maneira de andar. A entidade alega que o decreto invade matérias de competência privativa de lei, exorbitando os poderes normativos concedidos pela Constituição Federal ao presidente da República, e viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa.

4. CONSIDERAÇÕES FINAIS

Diante de todo o exposto acerca da atual legislação de proteção de dados pessoais no Brasil e das normas que disciplinam o tratamento desses dados, observa-se que a matéria ainda encontra-se num momento incipiente no ordenamento jurídico pátrio, devendo ainda ser tema de importantes debates – que inclusive possam vir a modificar o conjunto legal e normativo que se encontra em vigor. Ainda há que se analisar os impactos da efetiva implementação da Lei Geral de Proteção de Dados, especialmente após a entrada em vigor de suas sanções.

Igualmente, ainda é cedo para apontar todos os possíveis problemas e virtudes que advirão com seu efetivo encontro com a realidade fática. Todavia, é notável que há em cena uma antinomia de interesses que se apresenta pela comparação entre a LGPD e o Decreto de Bolsonaro – consubstanciado na criação de uma base nacional integradora de dados pessoais. Percebe-se que o atual governo federal tende a buscar um maior controle informacional da sociedade – tanto pela assinatura do decreto quanto pelos vetos presidenciais à LGPD.

Ainda que as justificativas governamentais apontem para uma melhora da prestação de políticas públicas, há que se atentar para os precedentes que estaremos abrindo ao permitir a instituição de tão ampla base de dados nas mãos de um governo central. O decreto assinado por Jair Bolsonaro reduziu barreiras e favoreceu o intercâmbio de

dados entre os poderes instituídos, enquanto calou sobre as salvaguardas à privacidade, segurança e proteção (limitando-se a excepcionar de sua incidência dados protegidos por sigilo bancário e fiscal). Estabelecendo condições normativas para que uma variedade de bases de dados fossem compartilhadas e cruzadas e ensejando, assim, usos de *Big Data* no âmbito da administração pública, o decreto falhou em prever limites a tais usos, endereçar os riscos à segurança associados e dispor sobre a proteção de dados.

São preocupantes as constatações de que falta rigor e precisão às definições do conjunto de informações potencialmente absorvidos pelo Cadastro Base do Cidadão – desafiando princípios e conceitos da lei geral. Tal fato revela que o interesse da administração pública com a assinatura deste decreto se dirigiu muito mais à consolidação de um sistema de controle e vigilância estatal, a despeito da promoção de direitos individuais e coletivos como a privacidade e a autodeterminação informativa.

Há certa imprecisão acerca da dimensão e do tipo de informação que passará a ser coletada pelo governo, bem como a sua destinação, o que pode vir a ocasionar grande insegurança jurídica. Até mesmo a maneira de andar do indivíduo passará a ser catalogada no âmbito dessa base integradora, elevando como nunca os níveis de vigilância estatal.

De qualquer maneira, a disciplina da lei geral possui maior força normativa e deverá prevalecer em face da regulação trazida pelo decreto presidencial. Desse modo, a coleta e o tratamento de dados no país deverão ficar ainda vinculados aos princípios expressos na LGPD, respeitadas as competências, atribuições, finalidades e responsabilidades nela previstas.

REFERÊNCIAS BIBLIOGRÁFICAS

ARENDDT, Hannah. **Origens do totalitarismo: anti-semitismo, imperialismo e totalitarismo**. Trad. de Roberto Raposo. São Paulo: Companhia das Letras, 1989.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

_____. **MEDIDA PROVISÓRIA Nº 869, DE 27 DE DEZEMBRO DE 2018**. Convertida na Lei nº 13.853, de 2019.

_____. **LEI Nº 13.853, DE 8 DE JULHO DE 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

_____. **DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

_____. **MEDIDA PROVISÓRIA Nº 954, DE 17 DE ABRIL DE 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo

RBHD, Rio de Janeiro, v.1, n. 2, Dossiê Temático 2, p. 100-125, jan./jun., 2021

Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

_____. **LEI Nº 14.010, DE 10 DE JUNHO DE 2020.** Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19).

_____. **DECRETO Nº 10.474, DE 26 DE AGOSTO DE 2020.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

CASTELLS, Manuel. **O poder da identidade.** São Paulo; Paz & Terra. 2010.

_____. **Ruptura: a crise da democracia.** Rio de Janeiro; Zahar. 2018.

CIPL; CEDIS-IDP. **O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD).** Documento integrante do Projeto Conjunto "Implementação e Regulamentação Efetiva da Nova Lei de Proteção de Dados brasileira". Abril, 2020.

COALIZÃO DIREITOS NA REDE. **Vigência da LGPD e os desafios na implementação da ANPD e do CNPD.** Publicado em 4 de setembro de 2020. Disponível em: <http://direitosnarede.org.br/2020/09/04/vigencia-da-lgpd-e-os-desafios-na-implementacao-da-anpd-e-docnpd/>

_____. **ANPD militarizada: risco para a proteção de dados pessoais.** Publicado em 16 de outubro de 2020. Disponível em <http://direitosnarede.org.br/2020/10/16/anpd-militarizada-risco-para-a-protecao-de-dados-pessoais>

_____. **CDR e Access Now enviam carta-denúncia para Comissão Europeia, Conselho da Europa e Global Privacy Assembly.** Publicado em 10 de novembro de 2020. Disponível em: <http://direitosnarede.org.br/2020/11/10/cdr-e-access-now-enviam-carta-denuncia-paracomissao-europeia-conselhoda-europa-e-global-privacy-assembly/>

CODING RIGHTS. **CADASTRO BASE DO CIDADÃO: A MEGABASES DE DADOS.** Dezembro de 2020. Disponível em: <https://medium.com/codingrights/cadastro-base-do-cidad%C3%A3o-a-megabase-de-dados-424bdaf7b06f>

COMISSÃO EUROPEIA. **A proteção de dados na UE: Autoridades Nacionais de proteção de dados.** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** 2. ed. rev., atual. e ampl. - São Paulo: Thomson Reuters Brasil, 2019.

DATA PRIVACY BRASIL. **Dadocracia – Episódio 33 – A hora e a vez da ANPD.** Publicado em 27 de outubro de 2020. Disponível em: <https://dataprivacy.com.br/dadocracia-episodio-33-a-hora-e-a-vez-da-anpd/>

_____. **Memória do Observatório: Episódio 4/2019: A saga da Autoridade.** In: Observatório Privacidade. Disponível em: <https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/>

DONEDA, Danilo. Da **privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados**. 2ª Ed. São Paulo: Thomas Reuters Brasil, 2019.

FRAGOSO, Nathalie; MASSARO, Heloisa. **Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina?** Publicado em 20/12/2019 em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/cadastro-base-e-amplo-compartilhamento-de-dados-pessoais-a-que-se-destina/>

FEIGELSON, Bruno; LEITE, Luiza. **ANPD – Autoridade autoritária de dados: Opção por órgão em vez de autarquia especial implica no enfraquecimento da instituição**. JOTA. Publicado em 1º de janeiro de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novastecnologias/anpd-autoridade-autoritaria-de-dados-01012019>

FRAGOSO, Nathalie; MASSARO, Heloisa. **Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina? A sina dos dados coletados pelo Estado brasileiro**. JOTA. Publicado em 19 de dezembro de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/cadastro-base-e-amplo-compartilhamento-de-dados-pessoais-a-que-se-destina-19122019>

HORNUNG, Gerrit; SCHNABEL, Christoph. **Data protection in Germany I: The population census decision and the right to informational self-determination**. *Computer Law & Security Review*, v. 25, n. 1.

KEMENY, Richard. **Brazil is sliding into techno-authoritarianism: Once a groundbreaker in internet governance, the country is becoming a surveillance state, thanks partly to covid- 19**. MIT Technology Review. Publicado em 19 de agosto de 2020. Disponível em: <https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/>

KOOPMANS, Ruud. **Movements and Media: Selection Processes and Evolutionary Dynamics in the Public Sphere**. *Theory and Society*, 33 (3/4):367-391 (2004). Disponível em <
<https://link.springer.com/article/10.1023%2FB%3ARYSO.0000038603.34963.de>>

MARANHÃO, Juliano; CAMPOS, Ricardo. **A divisão informacional de Poderes e o Cadastro Base do Cidadão: Decreto é uma verdadeira ‘carta branca’ para circulação irrestrita de dados, inclusive os de natureza pessoal, na Administração Pública**. JOTA. Publicado em 18 de outubro de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-ocadastro-base-do-cidadao-18102019>

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais: privacidade e responsabilidade civil**. Análise a partir do Marco Civil da Internet. *Revista Pensar*, v. 22, n. 1 2017.

MORAES, Maria Celina Bodin de. Apresentação. In: RODOTÁ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.

MULHOLLAND, Caitlin Sampaio. **Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: Uma Análise à Luz da Lei Geral De Proteção De Dados (Lei 13.709/18)**. *R. Dir. Gar. Fund.*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **A Normatividade dos Dados Sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana**. *Rev. de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Goiânia* | v. 5 | n. 1 | p. 63-85 | Jan/Jun. 2019.

OCDE. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. 2002. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>

RBHD, Rio de Janeiro, v.1, n. 2, Dossiê Temático 2, p. 100-125, jan./jun., 2021

OYAMA, Érico. **Especialistas dizem que ANPD precisará de autonomia e terá papel de coordenação: Autoridade Nacional de Proteção de Dados vai estabelecer parâmetros da LGPD; órgão ainda será criado.** JOTA. Publicado em 20 de agosto de 202. Disponível em: <https://www.jota.info/casa-jota/especialistas-dizem-que-anpd-precisara-de-autonomia-e-tera-papel-decoordenacao-20082020>

PORTAL G1. **OCDE pede que governo brasileiro garanta 'independência' de órgão de proteção de dados: ANPD será responsável por editar normas e fiscalizar cumprimento da lei de dados, em vigor desde setembro. OCDE pede mudanças na lei que vincula o órgão à Presidência da República.** Publicado por Luiz Felipe Bariéri em 26 de outubro de 2020. Disponível em: <https://g1.globo.com/politica/noticia/2020/10/26/ocde-pede-que-governo-brasileiro-garantaindependencia-de-orgao-de-protecao-de-dados.ghml>

REIA, Jhessica [et al.] [organizadores]. **Horizonte presente: tecnologia e sociedade em debate.** Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** privacidade hoje, Rio de Janeiro: Renovar, 2008.

SENADO FEDERAL. **Proposta de Emenda à Constituição nº 17, de 2019.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>

SUPREMO TRIBUNAL FEDERAL. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE.** Notícias STF. Publicado em 07 de maio de 2020. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>

UNESCO. **Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet.** Publicado em 2015 pela Organização das Nações Unidas para a Educação, Ciência e Cultura. Disponível em: <http://www.unesco.org/new/en/Internetstudy>

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** <http://data.europa.eu/eli/reg/2016/679/oj>

WARNER, Malcolm; STONE, Mike. **The data bank society: organizations, computers and social freedom.** Allen & Unwin, 1970.

ZUBOFF, Shoshana. **Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação.** Tecnopolíticas da vigilância: perspectivas da margem (Bruno, Cardoso, Kanashiro, Guilhaon e Melgaço (orgs.)). 2018. São Paulo: Boitempo.